UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/815,213	03/31/2004	Matthew Paul Duggan	AUS920040010US1	7107

34533   7590   11/25/2009
INTERNATIONAL CORP (BLF)
c/o BIGGERS & OHANIAN, LLP
P.O. BOX 1469
AUSTIN, TX 78767-1469

EXAMINER
KIM, JUNG W

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
11/25/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

office@biggerslaw.com
jennifer@biggerslaw.com
michelle@biggerslaw.com

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _10 August 2009_.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-28_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-28_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   This Office action is in response to the amendment filed on 8/10/09.

2.   Claims 1-28 are pending.

Response to Amendment

3.   The 101 rejections to claims 1-9 are withdrawn as the method is now tied to a particular machine.

Response to Arguments

4.   Applicant's arguments with respect to the 101 rejections of claims 19-28 are persuasive. These claims are directed to a computer program product embodied on a recordable computer-readable medium.

5.   Applicant's arguments with respect to the prior art rejections have been fully considered but are not persuasive.

6.   Applicant argues on pgs. 10-11 of the Remarks, that the applied prior art does not suggest the claimed limitations because the primary reference, Dunn, merely "links different identities in the same format." Remarks, pg. 10. Applicant points to col. 9 of the Dunn prior art in support of their argument. However, Dunn discloses two embodiments: one where multiple credentials are supported for a user in the same authentication system and one where multiple credentials are supported for a user across <u>federated authentication systems</u>. See col. 2, lines 48-54. As identified on col.

19, Dunn defines an embodiment of the invention whereby a user's identity on one

authentication system (i.e. a first security domain) is linked to the user's identity on a

different authentication system (i.e. a second security domain) ("In a federated scenario

example ..."). Hence, Dunn clearly discloses linking a user's identity across several

distinct security domains, which is clearly consistent with Applicant's invention as

defined in the specification. See Specification, pg. 1. ("A 'federation' is a collection of

security domains that have established trust. ... Entities within a federation often gain

access to resources in a first domain using security information in a native format for the

first domain (such as for example SAML), but to gain access to resources in a second

domain, the requesting entity often must provide security information in a native format

for the second domain ...").

7.   Furthermore, Applicant clarifies what is meant by their use of the phrase 'same

security information' on pg. 11 of the Remarks:

> By using the words same security information in Applicants' arguments,
> Applicants mean that the security information returned to the system entity
> in the native format of the second security domain is the equivalent of the
> security information security information [sic] in the native format of the
> first security domain which was translated to a canonical format,
> transformed, and translated in the native format of the second security
> domain.

8.   Based on this explanation, it appears that Applicant's bone of contention

regarding the Dunn prior art is the absence of a translation step from a native format of

a first domain to a canonical format, then to a native format of a second domain.

Hence, Applicant's arguments with respect to what Dunn lacks, is actually directed to

the combined teachings of Dunn and Bussler; after all, the rejection points to the

teachings of Bussler to suggest a translation step from a native format of a first domain

to a canonical format, then to a native format of a second domain using XML.

9.   With respect to the secondary prior art, Applicant argues that Bussler in

combination with the primary reference Dunn fails to suggest the features of the claimed

invention because Bussler only suggests taking the "transformed data in one direction

only, from source-side native phase to source-side application phase, from source-side

application phase, and so on. But there is no teaching or suggestion in Bussler of any

return from the target side to the source side." (Remarks, pg. 12) Applicant's argument

is not persuasive, because it does not take into consideration the combined teachings of

Dunn and Bussler. The question is not whether one reference or the other suggests a

claimed feature, but whether the combined teachings of the prior art suggest the

limitations in question. Dunn clear teaches "receiving from a system entity, in a security

service, security information in a native format of a first security domain regarding a

system entity having an identity in at least one security domain between two security

identity broker (Col. 19:17-35; see steps 2 and 3, supra); transforming the security

information including a value transformation for mapping a system's entity's identity in

the first security domain to another identity in the second security domain (steps 5-6)

and returning to the system entity the security information in the native format of the

second security domain (steps 7-8). Bussler teaches enabling two or more

heterogeneous applications to exchange communications with one another. In

particular, Bussler discloses translating a source-side native phase item to a source-

side application phase, and then to a common view phase item. The common view

phase item is then translated to a target-side application phase, and finally to a target-side native phase item. Col. 4:3-11. Hence, Dunn as modified by Bussler, suggest an invention where the <u>translation</u> of the user's security data from pageA.net to pageB.net occurs using a multiphase operation from a first domain native format to a canonical format and then to a second domain native format. Dunn's disclosure of returning the translated security identity (steps 7 and 8) back to the second security domain is still relevant in view of the modification by Bussler. Contrary to applicant's arguments that Bussler teaches away from the claimed invention (Remarks, pg. 15), nothing in Bussler suggest that the resulting operation cannot return the transformed data from the target side to the source side. Bussler's invention emphasizes the ability of heterogeneous applications to communicate with one another, rather than defining an invention that requires a strict flow of data from one entity to another. See col. 2:61-65. The key invention in Bussler is not to provide data from one entity to another entity, but to transform data from a first format particular to a first application to another format particular to a second application to <u>enable integration between the heterogeneous applications</u>. Furthermore, Bussler expressly discloses integrating a multistage transformation of data between heterogeneous applications to disburse the integration over several participants of the communication, and thereby reducing the complexity of the conversion. Col. 2:30-36. For these reasons, the independent claims remains rejected under the prior art of record.

10.   Finally, applicant's argument that the rejections to dependent claims 7-10, 16-18 and 26-28 should be withdrawn because neither Dunn nor Bussler disclose mappings

expressed in XSL, are not persuasive. As articulated in the rejections, "XSL is the

standard means of defining transformations of an XML file." See pg. 10, non-final

rejection mailed on 5/11/09. Applicant has not rebutted this fact, nor has Applicant

suggested that it would not be obvious to one of ordinary skill in the art of XML

translations to utilize XSL. Hence, merely because Bussler does not expressly disclose

using XSL does not overcome the basis for the rejection.

11.   For these reasons, applicant's claimed invention remains rejected under the prior

art of record.

Claim Rejections - 35 USC § 103

12.   Claims 1-28 are rejected under 35 U.S.C. 103(a) as being unpatentable under

Dunn et al. US 7,428,750 (hereinafter Dunn) in view of Bussler et al. USPN 7,072,898

(hereinafter Bussler).

13.   As per claims 1-9, Dunn discloses a computer-implemented method for cross

domain security information conversion (Abstract; col. 2:56-59), the computer

comprising a computer processor and a computer memory operatively coupled to the

computer processor, the computer memory having disposed within it computer program

instructions that execute the method, the method comprising:

        a.   receiving from a system entity, in a security service, security information in

        a native format of a first security domain regarding a system entity having an

identity in at least one security domain, wherein the system entity comprises

automated computing machinery (19:22-27; fig. 4, reference nos. 408 and 418);

b.   transforming the security information using a predefined mapping from a

first security domain to a second security domain, including value transformation

and mapping a system entity's identity in the first security domain to another

identity in the second security domain (19:29-31; fig. 2, reference no. 216);

c.   returning to the system entity the security information in the native format

of the second security domain (19:32-35; fig. 4, reference no. 416);

d.   wherein receiving security information further comprises receiving a

request for security information for the second security domain, wherein the

request encapsulates the security information in a native format of a first security

domain (19:20-23);

e.   wherein the system entity comprises a computer program product entity

requesting access to a resource in the second security domain (19:18-21; fig. 4,

reference nos. 402, 412 and 416);

f.   wherein the system entity comprises a computer program product entity

providing access to a resource in the second security domain (19:34-37; fig. 4,

reference no. 412).

14.   Dunn does not disclose translating the security information to a canonical format

for security information, wherein the canonical format is a data format for security

information that is standardized for user in data transformations of security information;

wherein transforming the security information includes transforming information in the

canonical format using a predefined mapping from the first security domain to a second

security domain; translating the transformed security information in the canonical format

to a native format of the second security domain; wherein transforming the security

information includes structure transformation; wherein translating the security

information in a native format of a first security domain to a canonical format comprises

a procedural software function; wherein translating the transformed security information

in the canonical format to a native format of the second security domain comprises a

procedural software function; and expressing the canonical format in XML, whereby

security information is translated between the first native format and the second native

format via the canonical format via XSL.

15.   Bussler discloses an method for exchanging communications between

heterogeneous applications wherein data items go through five processes between a

source and destination: 1) source-side native phase, 2) source-side application phase,

3) common view phase, 4) target-side application phase, and 5) target-side native

phase, whereby the source-side application phase, common view phase and target-side

application phase utilize XML to express the data from the source-side application to the

target-side application and vice versa. (3:60-4:43; 5:15-7:51) During the source-side

native phase, an item is received from a source application in its native form, wherein

the syntax, encoding and arrangement is particular to the source application; this item is

then converted to an application-independent syntax using "common" syntax such as an

XML document. (5:15-67) During the source-side application phase, elements in the

application-independent item are rearranged to convert the item into a common view

form. (6:1-34) During the common view phase, the all application-specific formatting

and encoding are eliminated to generate a canonical format. (6:38-60) The target-side

application phase and the target-side native phases are the corresponding reverse

phases to transform and translate the canonical format item to the native format item

corresponding to the target. (6:64-7:20) Furthermore, XSL is the standard means of

defining transformations of an XML file. Moreover, Bussler discloses that the invention

overcomes deficiencies of prior inventions, which centralize integration procedures, by

disbursing the integration over the several participants of the communication. (See 2:30-

36)

16.   Therefore, it would be obvious to one of ordinary skill in the art at the time the

invention was made for the program instructions stored on the computer program

product of Dunn when executed to cause the data processing system to carry out the

following steps: translating the security information to a canonical format for security

information, wherein the canonical format is a data format for security information that is

standardized for user in data transformations of security information; wherein

transforming the security information includes transforming information in the canonical

format using a predefined mapping from the first security domain to a second security

domain; translating the transformed security information in the canonical format to a

native format of the second security domain; wherein transforming the security

information includes structure transformation; wherein translating the security

information in a native format of a first security domain to a canonical format comprises

a procedural software function; wherein translating the transformed security information

in the canonical format to a native format of the second security domain comprises a

procedural software function; and expressing the canonical format in XML, whereby

security information is translated between the first native format and the second native

format via the canonical format via XSL. One would be motivated to do so to disburse

the integration over the several participants of the communication, thereby reducing the

complexity of the conversion (Bussler, 2:30-36)

17.   Finally, although neither Dunn nor Bussler expressly disclose the first and

second native format is expressed in XML, it is notoriously well known for a federation

native format to be expressed in XML. For example, SAML is an XML-based standard

for exchanging authentication and authorization data within a federation. Official notice

of this teaching is taken. It would be obvious to one of ordinary skill in the art at the time

the invention was made for the second native format to be expressed in XML. One

would be motivated to do so because SAML is a proven standard for exchanging

authentication and authorization data within a federation. The aforementioned cover the

limitations of claims 1-9.

18.   As per claims 10-18, Dunn discloses a system for cross domain security

information conversion (Abstract; col. 2:56-59), the system comprising a computer

processor operatively coupled to a computer memory, the computer memory having

disposed within it computer program instructions for:

   g.   receiving from a system entity, in a security service, security information in

        a native format of a first security domain regarding a system entity having an

identity in at least one security domain (19:22-27; fig. 4, reference nos. 408 and 418);

h.   transforming the security information using a predefined mapping from a first security domain to a second security domain, including value transformation and mapping a system entity's identity in the first security domain to another identity in the second security domain (19:29-31; fig. 2, reference no. 216);

i.   returning to the system entity the security information in the native format of the second security domain (19:32-35; fig. 4, reference no. 416);

j.   wherein receiving security information further comprises receiving a request for security information for the second security domain, wherein the request encapsulates the security information in a native format of a first security domain (19:20-23);

k.   wherein the system entity comprises a computer program product entity requesting access to a resource in the second security domain (19:18-21; fig. 4, reference nos. 402, 412 and 416);

l.   wherein the system entity comprises a computer program product entity providing access to a resource in the second security domain (19:34-37; fig. 4, reference no. 412).

19.   Dunn does not disclose instructions for translating the security information to a canonical format for security information; wherein transforming the security information includes transforming information in the canonical format using a predefined mapping from the first security domain to a second security domain; translating the transformed

security information in the canonical format to a native format of the second security

domain; wherein transforming the security information includes structure transformation;

wherein translating the security information in a native format of a first security domain

to a canonical format comprises a procedural software function; wherein translating the

transformed security information in the canonical format to a native format of the second

security domain comprises a procedural software function; and expressing the

canonical format in XML, whereby security information is translated between the first

native format and the second native format via the canonical format via XSL.

20.   Bussler discloses an apparatus for exchanging communications between

heterogeneous applications wherein data items go through five processes between a

source and destination: 1) source-side native phase, 2) source-side application phase,

3) common view phase, 4) target-side application phase, and 5) target-side native

phase, whereby the source-side application phase, common view phase and target-side

application phase utilize XML to express the data from the source-side application to the

target-side application and vice versa. (3:60-4:43; 5:15-7:51) During the source-side

native phase, an item is received from a source application in its native form, wherein

the syntax, encoding and arrangement is particular to the source application; this item is

then converted to an application-independent syntax using "common" syntax such as an

XML document. (5:15-67) During the source-side application phase, elements in the

application-independent item are rearranged to convert the item into a common view

form. (6:1-34) During the common view phase, the all application-specific formatting

and encoding are eliminated to generate a canonical format. (6:38-60) The target-side

application phase and the target-side native phases are the corresponding reverse

phases to transform and translate the canonical format item to the native format item

corresponding to the target. (6:64-7:20) Furthermore, XSL is the standard means of

defining transformations of an XML file. Moreover, Bussler discloses that the invention

overcomes deficiencies of prior inventions, which centralize integration procedures, by

disbursing the integration over the several participants of the communication. (2:30-36)

21.   Therefore, it would be obvious to one of ordinary skill in the art at the time the

invention was made to modify the invention of Dunn to further include instructions for:

translating the security information to a canonical format for security information;

wherein transforming the security information includes transforming information in the

canonical format using a predefined mapping from the first security domain to a second

security domain; translating the transformed security information in the canonical format

to a native format of the second security domain; wherein transforming the security

information includes structure transformation; wherein translating the security

information in a native format of a first security domain to a canonical format comprises

a procedural software function; wherein translating the transformed security information

in the canonical format to a native format of the second security domain comprises a

procedural software function; and expressing the canonical format in XML, whereby

security information is translated between the first native format and the second native

format via the canonical format via XSL. One would be motivated to do so to disburse

the integration over the several participants of the communication, thereby reducing the

complexity of the conversion (Bussler, 2:30-36)

22.   Finally, although neither Dunn nor Bussler expressly disclose the second native

format is expressed in XML, it is notoriously well known for a federation native format to

be expressed in XML. For example, SAML is an XML-based standard for exchanging

authentication and authorization data within a federation. Official notice of this teaching

is taken. It would be obvious to one of ordinary skill in the art at the time the invention

was made for the second native format to be expressed in XML. One would be

motivated to do so because SAML is a proven standard for exchanging authentication

and authorization data within a federation. The aforementioned cover the limitations of

claims 10-18.

23.   As per claims 19-28, Dunn discloses a computer program product for cross

domain security information conversion (Abstract; col. 2:56-59), the computer program

product embodied on a recordable computer-readable medium (3:51-4:14; 16:2-27), the

computer program product comprising program instructions, which when installed and

executed on a data processing system, are capable of causing the data processing

system to carry out the steps of:

> m.   receiving from a system entity, in a security service, security information in
>
> a native format of a first security domain regarding a system entity having an
>
> identity in at least one security domain, wherein the system entity comprises
>
> automated computing machinery (19:22-27; fig. 4, reference nos. 408 and 418);
>
> n.   transforming the security information using a predefined mapping from a
>
> first security domain to a second security domain, including value transformation

and mapping a system entity's identity in the first security domain to another

identity in the second security domain (19:29-31; fig. 2, reference no. 216);

o.   returning to the system entity the security information in the native format

of the second security domain (19:32-35; fig. 4, reference no. 416);

p.   wherein receiving security information further comprises receiving a

request for security information for the second security domain, wherein the

request encapsulates the security information in a native format of a first security

domain (19:20-23);

q.   wherein the system entity comprises a computer program product entity

requesting access to a resource in the second security domain (19:18-21; fig. 4,

reference nos. 402, 412 and 416);

r.   wherein the system entity comprises a computer program product entity

providing access to a resource in the second security domain (19:34-37; fig. 4,

reference no. 412).

24.   Dunn does not disclose translating the security information to a canonical format

for security information; wherein transforming the security information includes

transforming information in the canonical format using a predefined mapping from the

first security domain to a second security domain; translating the transformed security

information in the canonical format to a native format of the second security domain;

wherein transforming the security information includes structure transformation; wherein

translating the security information in a native format of a first security domain to a

canonical format comprises a procedural software function; wherein translating the

transformed security information in the canonical format to a native format of the second

security domain comprises a procedural software function; and expressing the

canonical format in XML, whereby security information is translated between the first

native format and the second native format via the canonical format via XSL.

25.   Bussler discloses an apparatus for exchanging communications between

heterogeneous applications wherein data items go through five processes between a

source and destination: 1) source-side native phase, 2) source-side application phase,

3) common view phase, 4) target-side application phase, and 5) target-side native

phase, whereby the source-side application phase, common view phase and target-side

application phase utilize XML to express the data from the source-side application to the

target-side application and vice versa. (3:60-4:43; 5:15-7:51) During the source-side

native phase, an item is received from a source application in its native form, wherein

the syntax, encoding and arrangement is particular to the source application; this item is

then converted to an application-independent syntax using "common" syntax such as an

XML document. (5:15-67) During the source-side application phase, elements in the

application-independent item are rearranged to convert the item into a common view

form. (6:1-34) During the common view phase, the all application-specific formatting

and encoding are eliminated to generate a canonical format. (6:38-60) The target-side

application phase and the target-side native phases are the corresponding reverse

phases to transform and translate the canonical format item to the native format item

corresponding to the target. (6:64-7:20) Furthermore, XSL is the standard means of

defining transformations of an XML file. Moreover, Bussler discloses that the invention

overcomes deficiencies of prior inventions, which centralize integration procedures, by

disbursing the integration over the several participants of the communication. (2:30-36)

26.   Therefore, it would be obvious to one of ordinary skill in the art at the time the

invention was made for the program instructions stored on the computer program

product of Dunn when executed to cause the data processing system to carry out the

following steps: translating the security information to a canonical format for security

information; wherein transforming the security information includes transforming

information in the canonical format using a predefined mapping from the first security

domain to a second security domain; translating the transformed security information in

the canonical format to a native format of the second security domain; wherein

transforming the security information includes structure transformation; wherein

translating the security information in a native format of a first security domain to a

canonical format comprises a procedural software function; wherein translating the

transformed security information in the canonical format to a native format of the second

security domain comprises a procedural software function; and expressing the

canonical format in XML, whereby security information is translated between the first

native format and the second native format via the canonical format via XSL. One

would be motivated to do so to disburse the integration over the several participants of

the communication, thereby reducing the complexity of the conversion (Bussler, 2:30-

36)

27.   Finally, although neither Dunn nor Bussler expressly disclose the second native

format is expressed in XML, it is notoriously well known for a federation native format to

be expressed in XML. For example, SAML is an XML-based standard for exchanging

authentication and authorization data within a federation. Official notice of this teaching

is taken. It would be obvious to one of ordinary skill in the art at the time the invention

was made for the second native format to be expressed in XML. One would be

motivated to do so because SAML is a proven standard for exchanging authentication

and authorization data within a federation. The aforementioned cover the limitations of

claims 19-28.

Conclusion

28.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

29.   Lai US 20050044197 discloses cross domain single sign-on across federated

authentication systems using XML.   See pgs. 66-68 (paragraphs 1277-1301)

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy

as set forth in 37 CFR 1.136(a).

         A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to JUNG KIM whose telephone number is (571)272-3804.

The examiner can normally be reached on FLEX.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll-free).

/Jung Kim/
Primary Examiner, AU 2432